

Appl. No. : 09/965,968
Filed : September 26, 2001

AMENDMENTS TO THE CLAIMS

IN THE CLAIMS:

A complete set of claims is provided below.

Please cancel Claims 10-12.

Please amend Claims 13, 18, and 22 as indicated below.

1.-12. (Canceled)

13. (Currently Amended) An anti-alteration system for web-content, comprising:

a public-web-server configured to store safe-web-files encrypted from original web-content including one or more types of static files and one or more types of dynamic files, and configured to provide HTTP web server functions;

a private-web-server configured to store said original web-content, said private-web-server provided to said public-web-server through a firewall, said firewall configured to block all Internet communication such that files in said private web server cannot be accessed from the Internet, rather, said firewall configured to pass recovery requests from said public-web-server to said private-web server;

wherein when a web visitor's request is received, said public-web-server is configured to verify that said safe-web-file has not been improperly altered, deleted or replaced, said public-web-server further configured to decrypt one or more of said safe-web-files and respond to said visitor; and

said public-web-server further configured to automatically send a recovery request to said private-web-server when said public-web-server detects an unauthorized alteration of said safe-web-files, said private-web-server, in response to said recovery request, configured to create new safe-web-files by encrypting one or more files of said original-web-content and send said new safe-web-files to said public server through said firewall.

14. (Previously presented) The anti-alteration system, as recited in Claim 13, wherein said encryption comprises chaos encryption technology to do encryption and decryption of said web-content for increasing the web server response speed and increasing security strong of whole system.

Appl. No. : 09/965,968
Filed : September 26, 2001

15. (Previously presented) The anti-alteration system, as recited in Claim 13, further comprising a real-time-check module used on said public-web-server computer for linking to a decryption module, wherein said decryption module is configured to decrypt one or more of said safe-web-files in response to an HTTP request received from said web visitor.

16. (Previously presented) The anti-alteration system as recited in Claim 15, further comprising a real-time-check module configured to use symmetric-key encryption to decrypt one or more of said safe-web-files when said web visitor's request is received.

17. (Previously presented) The anti-alteration system, as recited in Claim 16, wherein said symmetric-key encryption is selected from a group consisting essentially of DES, 3DES and AES.

18. (Currently Amended) An anti-alteration system for web-content, comprising:
a public-web-server configured to store safe-web-contents that have been provided with header information including a MAC (Message Authentication Code) generated from said original web-content, and properties of said original-web-content including, name, size, date, and location thereof;

a private-web-server configured to store said original web-content said public-web-server provided to said private-web-server through a firewall, said firewall configured to pass recovery requests from said public-web-server to said private-web server, said firewall configured to block other communication from the public-web-server to the private-web-server such that web content files in said private web server cannot be accessed from the Internet;

said private-web-server configured to separate said header information from a requested safe-web-file , and using said MAC (Message Authentication Code) included in said header information to check an authenticity of said safe-web-file; and

said public-web-server configured to add new header information to said original web-content to create a new safe-web-file on said private-web-server computer when an unauthorized alteration of said safe-web-file is detected, wherein said new safe-web-file is sent to said public-web-server computer to automatically restore said altered safe-web-file.

Appl. No. : 09/965,968
Filed : September 26, 2001

19. (Previously presented) The anti-alteration system, as recited in Claim 18, further comprising a real-time-check module used on said public-web-server computer for linking to an authentication module, wherein said authentication module is configured to provide authentication of said safe-web-file in response to a request received from said web visitor though http protocol.

20. (Previously presented) The anti-alteration system, as recited in Claim 19, wherein said real-time-check module uses a message authentication technology using chaos theory to check whether the safe-web-content has been altered.

21. (Previously presented) The anti-alteration system, as recited in Claim 18, wherein said real-time-check module that is configured to link said public-web-server services by using at least one message authentication technology selected from a group consisting essentially of MD4, MD5, and SHA.

22. (Currently Amended) An anti-alteration system for web-content, comprising:
a public-web-server computer, configured to store safe-web-files which have been encrypted from original web-contents and have been provided with header information, said header information including a MAC (Message Authentication Code) generated from authentication checking said original web-content and properties including name, size, date, and storage location thereof;
a private-web-server computer which retains said original web-content and which is provided to said public-web-server computer through a firewall;
a real-time-check module, in response to a web visitor's request safe-web file, said real-time-check module configured to separate said header information from said safe-web-file and using a MAC (Message Authentication Code) included in said header information to authenticate said safe-web-file by comparing said header information with;
separate header information; and
a recovery module, when an unauthorized alteration of said safe-web-file is detected, said recovery module configured to encrypt said original web-content and add header information to said original web-content to create a new safe-web-file on said private-web-server computer, sending said new safe-web-file to said public-web-server computer to automatically restore said safe-web-file which has been altered, said private-web-server

Appl. No. : 09/965,968
Filed : September 26, 2001

protected by a firewall module configured to pass recovery requests from said public-web-server to said private-web server, said firewall module configured to block other communication from the public-web-server to the private-web-server such that files in said private web server cannot be accessed from the Internet.

23. (Previously presented) The anti-alteration system, as recited in Claim 22, wherein said recovery module uses chaos encryption technology to do encryption and decryption.

24. (Previously presented) The anti-alteration system, as recited in Claim 22, wherein said real-time-check module is configured to provide authentication of said safe-web-file in response to a request received from said web visitor through http protocol.

25. (Previously presented) The anti-alteration system, as recited in Claim 23, wherein said real-time-check is configured to use a symmetric-key encryption to decrypt said safe-web-contents in response to said web visitor's request.

26. (Previously presented) The anti-alteration system, recited in Claim 25, wherein said symmetric-key encryption is selected from a group consisting essentially of DES, 3DES, RC4 and AES.

27. (Previously presented) The anti-alteration system, as recited in Claim 24, wherein said real-time-check module uses a message authentication technology using chaos theory to check whether the safe-web-content has been altered.

28. (Previously presented) The anti-alteration system, as recited in Claim 24, wherein said real-time-check module uses at least one of MD4, MD5, and SHA for message authentication.